UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/696,200	10/28/2003	David M. Chess	GB920030050US1	7325

26502 7590 12/21/2006

IBM CORPORATION
IPLAW IQ0A/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
HOANG, DANIEL L	

ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/21/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/696,200	CHESS ET AL.	
	Examiner	Art Unit	
	Daniel L. Hoang	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/28/03*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/28/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-14 are rejected under 35 U.S.C. 102(b) as being anticipated by Grimm et al., US Patent No. 6,317,868, hereinafter Grimm.

As per claim 1, 8 and 14 Grimm teaches:

A method for detecting malicious software within or attacking a computer system, said method comprising the steps of:

> *[see column 8, lines 56-60] "the present invention readily enables administrators and users of computer systems to enforce site specific security policies on software components by applying access control, protection domains, and auditing trails."*

in response to a system call, executing a hook routine at a location of said system call to

> *[see column 4, lines 23-27] "When software component 11 as originally created needs to be loaded for execution by a computer, the present invention provides an introspection service 13 that intercepts the software component for analysis."*

(a) determine a data flow or process requested by said call,

> *[see above, "original software component 11 needed to be loaded for execution."]*

(b) determine another data flow or process for data related to that of said call,

> *[see column 4, lines 65-67 and column 5, lines 1-2] "a component system (i.e., a computer or workstation) to which the original software component was directed for execution issues a command to load the software component for execution. Instead, the original software component is loaded and parsed as indicated in a block 12."*
>
> *[see column 6, lines 17-20] "A call is made to the component operation in a block 100. The modified software component invokes enforcement service 19 before the original component operation is executed."*

(c) automatically generate a consolidated information flow diagram showing said data flow or process of said call and said other data flow or process, and after steps (a-c),

> *[see column 7, lines 27-31] "A positive response to either of decision blocks 140 or 160 causes an audit record to be created in a block 142 or in a block 162, respectively. In the event that an audit record is necessary, one is created that lists the component operation, its arguments, any access control checks, and their results."*

(d) call a routine to perform said data flow or process requested by said call.

> [see column 6, lines 6-9] "*After a modified software component has been loaded (i.e., linked and activated) by a component system, it executes on the component system in the same manner it would have prior to modification by the present invention.*"

As per claim 2, Grimm teaches:

A method as set forth in claim 1, wherein a user monitors said information flow diagram and compares the data flow or process of steps (a) and (b) with a data flow or process expected by said user.

> *[see column 6, lines 58-63] "The enforcement service then performs access checks on each argument, or object, to be passed to the component operation. Each of these tests is made by querying the security policy service with the security identifier of the subject and the security identifier of the object to be checked."*

As per claim 3 and 9, Grimm teaches:

A method as set forth in claim 1, wherein said information flow diagram illustrates locations of said data at stages of a processing activity.

> *[see above, "A positive response to either of decision blocks 140 or 160 causes an audit record to be created in a block 142 or in a block 162, respectively."]*

The audit trail is can be created at blocks 142 and 162 of the process.

As per claim 4 and 10, Grimm teaches:

A method as set forth in claim 1, wherein said system call is selected from the set of: open file, copy file to memory, copy memory to register, mathematical functions, write to file, and network or communication functions.

[see column 4, lines 27-34] "Based upon information determined by introspection service 13, a security policy service 15 instructs an interposition service 17, which is also included in the present invention, how to modify the original software component to adhere to the security policies of the site."

As per claim 5 and 11, Grimm teaches:

A method as set forth in claim 1, wherein said system call is a software interrupt of an operating system.

[see column 4, lines 27-34] "Based upon information determined by introspection service 13, a security policy service 15 instructs an interposition service 17, which is also included in the present invention, how to modify the original software component to adhere to the security policies of the site."

As defined by applicant's specification, a software interrupts are program generated interrupts that stop the current processing in order to request a service provided by an interrupt handler. Grimm's invention teaches that the original software component is stopped of its current activity and modified as seen above.

As per claim 6 and 12, Grimm teaches:

A method as set forth in claim 1, wherein said system call causes a processor to stop its current activity and execute said hook routine.

[see rejection of claim 1 wherein the software component is intercepted.]

As per claim 7 and 13, Grimm teaches:

A method as set forth in claim 1 wherein said system call is made by malicious software.

[see column 7, lines 63-67] "the security policy service returns the appropriate access mode, and enforcement service 19 determines whether the returned access mode includes the specified access mode. If the returned access mode includes the specified access mode, then the check is successful."

CONCLUSION

The following patents and publications are cited to further show the state of the art with respect to systems for detecting and preventing malicious software.

US Patent No. 6,081,897, to Bersson, which is cited to show a system for monitoring and preventing unauthorized copying of data.

US PGP No. 20040107361 to Redan et al, which is cited to show a system for high speed network intrusion detection.

US PGP No. 20020174359 to Haltmeyer, which is cited to show thorough operation restriction.

US Patent No. 6,718,414 to Doggett, which is cited to show function modification in a write protected operating system.

US Patent No. 6,584,501 to Cartsonis et al., which is cited to show a method to display information representing network traffic on a computer display monitor.

US Patent No. 6,678,734 to Haatainen, which is cited to show a method for intercepting network packets in a computing device.

US Patent No. 6,021,437 to Chen et al., which is cited to show a system for real time monitoring of a data processing system.

*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Daniel L. Hoang

12/15/06

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

12/15/06